REMARKS

The Examiner has rejected Claims 1, 3-11, 13-19, 30, and 31-35 under 35 U.S.C. 103(a) as being unpatentable over Vaidya (U.S. Patent No. 6,279,113 B1), in view of Li et al. (U.S. Patent No. 6,567,408 B1). Further, the Examiner has rejected Claims 20-29 under 35 U.S.C 103(a) as being unpatentable over Copeland, III (U.S. Publication No. 2002/0144156 A1), in view of Li et al (U.S. Patent No. 6,567,408 B1). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended independent Claims 1 and 30 to at least substantially include the subject matter of former dependent Claims 10 and 11.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the *prima facie* case of obviousness and, in particular, the obviousness of combining the Vaidya and Li references, the Examiner argues that "it would have been obvious…to employ the teachings of Li within the system of Vaidya in order to enhance the performance and efficiency of the system." Applicant disagrees and respectfully asserts that it would not have been obvious to combine the teachings of the Vaidya and Li references, especially in view of the vast evidence to the contrary.

For example, Vaidya relates to an intrusion detection system, while Li relates to a system for classifying packets for providing a plurality of different levels of service. To simply glean features from a packet classification system, such as that of Li, and combine the same with the *non-analogous art* of intrusion detection systems, such as that of Vaidya, would simply be improper. The packet classification system of Li simply classifies packets for providing different levels of quality of service over a network, whereas the intrusion detection system of Vaidya detects packets associated with a network intrusion. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems the packet classification system of Li addresses, which merely relate to quality of service, as opposed to the intrusion detection system of Vaidya, the Examiner's proposed combination is inappropriate.

In addition, with respect to the obviousness of combining the Li and Copeland references, the Examiner argues that "it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Li within the system of Copeland in order to enhance the performance and efficiency of the system." Applicant disagrees and respectfully asserts that it would not have been obvious to combine the teachings of the Copeland and Li references, especially in view of the vast evidence to the contrary.

For example, Copeland relates to a method for detecting unauthorized network usage based upon port profiling, while Li relates to a classification method for classifying packets. To simply glean features from a port profiler, such as that of Copeland, and combine the same with the *non-analogous art* of a packet classifier, such as that of Li, would simply be improper. In particular, the port profiler of Copeland merely detects unauthorized usage (Copeland, Abstract), while the packet classifier of Li simply

classifies packets for providing different levels of quality of service over a network (Li, Abstract). In view of the vastly different types of problems a port profiler addresses as opposed to a packet classifier, the Examiner's proposed combination is inappropriate.

Thus, applicant respectfully asserts that the first element of the *prima facie* case of obviousness has not been met, as noted above. More importantly, applicant also respectfully asserts that the third element of the *prima facie* case of obviousness has not been met by the prior art references relied on by the Examiner. For example, with respect to independent Claim 20, the Examiner has relied on paragraphs [0157]-[0159] and [0163]-[0165] from the Copeland reference to make a prior art showing of applicant's claimed "detection engine operable to perform a table lookup at the flow table to select an action to be performed on said classified packets based on the classification, wherein comparing said classified packets to at least a subset of the signature profiles is one of the actions" (as currently amended).

Applicant respectfully asserts that the excerpts relied on by the Examiner merely disclose that "the flow collector thread…searches linearly through the entire flow data structure … to find flows that have been inactive for a certain time period" after which "a logic tree analysis is done to classify [the inactive flows] as either a normal flow, or a potential probe or other suspicious activity" (paragraph [0157] – emphasis added). Further, the excerpts teach that "[t]he packet classifier thread 610 collects information on network operations such as packets and bytes" and that "[t]he alert manager thread 630 writes the updated data to various output files for use by the user interface" (paragraph [0165] – emphasis added).

However, merely teaching the classification of inactive flows and the writing of updated data to output files fails to teach "a detection engine operable to perform a table lookup at the flow table to select an action to be performed on said classified packets based on the classification" and does not even suggest "comparing said **classified** packets to at least a subset of the signature profiles" (emphasis added), as claimed by applicant. Clearly, classifying inactive flows, as in Copeland, fails to meet "select[ing] an action to

be performed on said packet based on its classification" (emphasis added), in the manner as claimed by applicant.

Applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, since it would not have been obvious to combine the prior art references, and since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of former dependent Claims 10 and 11 into independent Claims 1 and 30.

With respect to the subject matter of former Claims 10 and 11 (now at least substantially incorporated into independent Claims1 and 30), the Examiner has relied on Col. 7, lines 2-11 and Col. 9, lines 27-35 of the Vaidya reference to make a prior art showing of applicant's claimed "performing a table lookup to select an action to be performed on said classified packets based on the classification" and technique "wherein one of the actions is comparing said classified packets to at least a subset of the signature profiles."

Applicant respectfully asserts that the excerpts from Vaidya relied on by the Examiner simply teach that "[i]f a network intrusion is detected, the reaction module is notified" (Col. 7, lines 6-7) and that "[t]he reaction module… takes steps to trace the application session associated with the data packet, to terminate the session, and/or to notify the network administrator" (Col. 7, lines 8-11 – emphasis added). However, merely teaching notifying a reaction module that can trace the session, terminate the session, and notify the network administrator fails to teach any sort of table lookup, let alone specifically "performing a table lookup to select an action to be performed on said classified packets based on the classification" (emphasis added), as claimed by applicant. Clearly, the reaction module that can trace and terminate the session fails to meet "select[ing] an action to be performed on said classified packets **based** on the classification" (emphasis added), in the manner as claimed by applicant.

Furthermore, the excerpts from Vaidya relied on by the Examiner simply teach that "building the instruction cache 42 includes the step 112 of creating a hash index based on the server IP address and the application information in the register cache 40" (Col. 9, lines 27-30 - emphasis added). In addition, Vaidya teaches that "the hash index is used to search the signature profile memory 39 for a set of attack signature profiles corresponding to the server and application associated with the packet information" (Col. 9, lines 33-36 – emphasis added) where "[i]f the search identifies a corresponding profile, the attack signature profiles signatures are imported into the instruction cache in step 120" (Col. 9, lines 43-45 – emphasis added).

However, the mere disclosure of creating a hash index which is used to search for attack signature profiles corresponding to the server and application associated with the packet information in order to import profile signatures into the instruction cache, as in Vaidya, fails to teach classified packets, and especially not "comparing said classified packets to at least a subset of the signature profiles" (emphasis added), as claimed by applicant. Clearly, searching a hash index for server IP address and application information fails to meet "comparing said classified packets," in the manner as claimed by applicant.

Again, applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met, as noted above. Thus, a notice of allowance or proper prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P318/01.240.01).

Respectfully submitted,
Zilka-Kotab, PC.

/KEVINZILKA/

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100